EXHIBIT A

United States Department of Justice
Criminal Division

Child Exploitation and Obscenity Section
High Technology Investigative Unit

Subject: Computer Forensic Examination – Investigation of David Bartels	
Examiner: Dero Tucker	**ACTS Number:** 202300569
Case Type: Child Exploitation	**Report Date:** December 4, 2023
Attachments: 21	**Page:** 1 of 7

ITEMS TO BE EXAMINED:

1. "**WDElements5TB_EXT.E01**" is a forensic image copy of a 5TB Western Digital Elements 2620 external hard drive with serial number WXQ2E60AE7UU and product number WDBU6Y0050BBK; MD5 hash b4c5b4676efc927f45b50 fba97388d11; created by Digital Investigative Analyst (DIA) Dero Tucker on June 28, 2023.

2. "**MSILaptop_1TBSamsung860EVO.E01**" is a forensic image copy of a 1TB Samsung V-NAND SSD 860 EVO with serial number S3Z8NB0KB39844N and model number MZ-76E1T0; MD5 hash f8b5eed326f64b6dd564a5caa 67b5483; created by DIA Dero Tucker on March 21, 2023.

3. "**DellLaptop_ToshibaHD1TB.E01**" is a forensic image copy of a 1TB Toshiba hard drive with serial number 86FRTL1BT, removed from a Dell laptop with service tag FZS9PC2; MD5 hash 01aa27c4a90cfea51e1fdde 65ad28fd3acd80dcb; created by DIA Dero Tucker on March 21, 2023.

4. "**EXTRACTION_FFS.zip**" is a full file system extraction of a Samsung Galaxy Z Fold 3 (SM-F926U1) with IMEI 356664830650753; MD5 hash value 5c88fe2dce19d9aab1ae3f09e4a9d104; created by DIA Dero Tucker on March 22, 2023.

5. "**WDMyPassport2TB_EXT.E01.E01**" is an image copy of a 2TB Western Digital My Passport external hard drive with serial number WX71A63T0022; MD5 hash of ef2d8ce71f6665c7fc32f37cb510af50; created by DIA Dero Tucker on March 21, 2023.

6. "**MSILaptop_1TBIntelNVME_1.E01**" is an image copy of a 1TB Intel SSD 660P Series NVME drive with serial number BTNH94241A361P0B, removed from a MSI laptop with serial number K1812N0018042; MD5 hash of 98f695c1dfae39706a2ad9a8cb9b075b; created by DIA Dero Tucker on March 21, 2023.

7. "**MSILaptop_1TBIntelNVME_2.E01**" is an image copy of a 1TB Intel SSD 660P Series NVME drive with serial number BTNH94241A361P0B, removed from a MSI laptop with serial number K1812N0018042; MD5 hash of 98f695c1dfae39706a2ad9a8cb9b075b; created by DIA Dero Tucker on March 21, 2023.

8. "**FujiFilmUSBDrive_16GB.E01**" is an image copy of a 16GB FujiFilm USB drive with MD5 hash ac7f8e9f4db5de7 acd567494725508ec; created by DIA Dero Tucker on March 22, 2023

9. "**61ac799cde43878ac28c419eced7855507196fd0_files_full.zip**" is a full file system extraction of an Apple iPad Mini 3 with serial number DLXNJ023G5V4; MD5 hash value fb924f109646c1b8fe8c4921dc059fcf; created by DIA Dero Tucker on March 21, 2023.

Subject: Computer Forensic Examination – Investigation of David Bartels	
Examiner: Dero Tucker	**ACTS Number:** 202300569
Case Type: Child Exploitation	**Report Date:** December 4, 2023
Attachments: 21	**Page:** 2 of 7

10. "**BOBLOV_SanDiskMicroSD256GB.E01**" is an image copy of a 256GB SanDisk Ultra SD card removed from a BOBLOV camera; MD5 hash 7640dbbe5edaaeebd865bcebfa2b5636; created by DIA Dero Tucker on June 28, 2023.

11. "**CleaningUpInLaundromatsCD.iso**" is a copy of an optical disk created by DIA Dero Tucker on June 28, 2023.

12. "**WDEasyStore_5TB.E01**" is an image copy of a Western Digital EasyStore external hard drive with serial number WX31E690SZCS; MD5 hash 98e8144f7b60adda7082a89fe8132497; created by DIA Dero Tucker on May 16, 2023.

13. "**Kingston128GB_NVME.E01**" is an image copy of a Kingston 128GB NVME Drive with ID SNS8154P3, removed from a NVME enclosure with serial number 2799-A17948; MD5 hash 8c8373ce75602ff31ad860e08cd2cbfc; created by DIA Dero Tucker June 28, 2023.

14. "**SanDiskMicroSD2GB.E01**" is an image copy of a 2GB microSD card with MD5 hash 9d914c772d2cb3676d1e4 471ba36ec38; created by DIA Dero Tucker on March 22, 2023.

15. "**MicroSD_15GB.E01**" is an image copy of a 15GB MicroSD Card with the ID Z16GE15 MDS2040156; MD5 hash 11aabe1b0697270cff76230db5863a08; created by DIA Dero Tucker on March 21, 2023.

16. "**SanDiskMicroSD128GB.E01**" is an image copy of a 128GB SanDisk Extreme MicroSD with MD5 hash b975067 8d0eb979f6e73df91dfc89aa1; created by DIA Dero Tucker on March 22, 2023.

17. "**SanDiskExtremeProSDCard_32GB.E01**" is an image copy of a 32GB SanDisk Extreme Pro with MD5 hash 011c442932d87fd389826a5882f9feea; created by DIA Dero Tucker on March 22, 2023.

18. "**WD14TB_WDElementsEXT.E01**" is an image copy of a 14TB Western Digital hard drive with serial number Y5KYP6JC; removed from a Western Digital Elements enclosure with model number WDBWLG0140HBK; MD5 hash 7d83e9873ea72776c9959c46607e7d00; created by DIA Dero Tucker.

EXAMINATION REQUESTED:

Verbal Command Authorized Search and Seizure granted by Captain Samuel White, USN, Commanding Officer, Naval Station Guantanamo Bay on January 5, 2023, providing authority to search seizure evidence in connection to Child Sexual Abuse Material.

FINDINGS:

ITEM 1: WDElements5TB_EXT (Western Digital 5TB External Hard Drive)

1. **Deeper Folder**
   The folder "\NSFW\Nope\Dont open\You were Warned\Deeper\" contains additional subfolders, such as "Telegram Desktop", "Apr21", and "Pluto666". The folder "Deeper" and its subfolders contain 41,026 images and videos, including images and videos depicting Child Sexual Abuse Material (CSAM), such as "804724626_237729.jpg", "Lolitashouse_[redacted]_12Yo_&_[redacted]_11Yo_Lesbian_Girls_Part_4_x264.mp4", and "[redacted]-bondage.avi". The images and videos within the folder "Deeper" and its subfolder contain a file creation date ranging between January 11, 2021 and April 18, 2021. **Attachment 1** contains the 41,026 images and videos

within the folder "Deeper" and its subfolders. A listing of attributes, such as the "File Name", "Logical Size", "File Created", "MD5 Hash", and "Item Path" for these images and videos are included in **Attachment 2**.

2. **Downloads Folder**
The folder "Downloads" contains 12 files, including seven Portable Document Format (.pdf) files. Some of these .pdf files are "AutoIDCard.pdf", "673.pdf", and "file.pdf". A review of these files identified the existence of the text "DAVID MARK BARTELS", "David Bartels", and "BARTELS, DAVID M". The file "673.pdf" also includes a Social Security number. The file creation date for the 12 files within the folder "Downloads" is September 23, 2021. **Attachment 3** includes the 12 files stored within the folder "Downloads". A listing of attributes, such as the "File Name", "Logical Size", "File Created", "MD5 Hash", and "Item Path" for these 12 files are included in **Attachment 4**.

ITEM 2: MSILaptop_1TBSamsung860EVO (MSI Laptop)

3. **JumpLists**
JumpLists are a Microsoft Windows feature that provides the user quick access to recently opened files for specific applications in the Windows Task Bar. Starting with Windows 7, Microsoft Windows operating system automatically create jumplist entries when user opens a file. These jumplist entries are stored in container files with filenames corresponding to their unique Application ID (AppID). The jumplist entries contain information about the opened or viewed file or folder, including the application used, filename, path location, volume name, and date and time attributes. These records remain even when the target file or folder is removed.

The subfolders "AutomaticDestinations" and "CustomDestinations" were located in the folder "\Users\dbart\AppData\Roaming\Microsoft\Windows\Recent\" and contained 39 jumplist container files. A review of the jumplists identified jumplist entries that contain filenames indicative of being CSAM, such as "G:\NSFW\Nope\Dont open\You were Warned\Deeper\9\1st-Studio Siberian Mouse Custom (NK_008).mp4", "G:\NSFW\Nope\Dont open\You were Warned\Deeper\new shit\New folder\(Pthc) 10Yo Straight Sex New 0607 - 8m42s.mp4", and "F:\NSFW\Nope\Dont open\You were Warned\Deeper\6\(opva)Buratino RA-04_NEW 2011 Pthc-Ptsc_x264 (1).mp4". The majority of the video files were accessed using the application VLC Player and still exist on the Western Digital 5TB External Hard Drive (Item 1). VLC Player is an application that allow the computer user to open and view video files.

Attachment 5 contains the 39 jumplist container files. **Attachment 6** contains the list of viewed files extracted from the jumplist container files.

4. **Microsoft Internet Explorer/Microsoft Edge**
Microsoft Internet Explorer and Microsoft Edge are applications included with the Microsoft Windows operating system and used to access websites on the internet and files stored on the computer. Microsoft Internet Explorer and Microsoft Edge store information about websites and files accessed by the computer user within the files "WebCachev01.dat" and "History". These files were located in the folders "\Users\dbart\AppData\Local\Microsoft\Windows\WebCache\" and "\Users\dbart\AppData\Local\Microsoft\Edge\User Data\Default\". The files "WebCachev01.dat" and "History" are included as **Attachment 7**. **Attachment 8** contains the extracted web browsing and file access activity.

A review of the file "WebCacheV01.dat" identified web browsing and file access activity ranging between June 4, 2022 and December 31, 2022. Some of the web browsing activity contain access to files within subfolders of the folder "Deeper", such as "G:/NSFW/Nope/Dont open/You were Warned/Deeper/Apr21 /Lolitashouse[redacted]_12Yo_&_[redacted]_11Yo_Lesbian_Girls_Part_4_x264.mp4", "\G:/NSFW/Nope/Dont

open/You were Warned/Deeper/Apr21/A wild hebe appears.mp4", and "G:/NSFW/Nope/Dont open/You were Warned/Deeper/Pluto666/Lesvianas/cp dos niñas en la sala y después en la ducha.mp4".

5. **Connected USB Devices**
The Microsoft Windows operating system stores information about Universal Serial Bus (USB) devices, such as a thumb drive or an external hard drive, that have been connected to the associated computer. This information includes device name, serial number, last connected date and time, first install date and time, and last assigned drive letter. The Microsoft Windows operating system stores this information within the Windows Registry. The Windows Registry is a database containing a series of configuration settings and data for the Microsoft Windows operating system, user accounts, and applications installed on the computer. A review of the registry key "USBSTOR" identified USB devices that were inserted into the computer. One of the USB device entries contain the label "WD Elements 2620 USB Device", with a last connected date of December 31, 2022. The USB device "WD Elements 2620" is the same make, model, and USB serial number as the Western Digital 5TB External Hard Drive (Item 1). **Attachment 9** contains the listing of connected USB devices extracted from the Windows Registry.

6. **Prefetch**
The Microsoft Windows operating system creates and use Prefetch files to increase the speed in which applications run. The Prefetch files can provide insight into what applications were run, application run count, and the date and time of the most recent application usage. Microsoft Windows 8 and above is capable of containing time and date of the last eight times an application was run. The folder "\Windows\Prefetch\" contains 387 Prefetch files with file creation dates ranging between October 04, 2022 and January 4, 2023. A review of this folder identified the Prefetch files "DISCORD.EXE-8D275F27.pf", "DISCORD.EXE-E4638A6C.pf", "TELEGRAM.EXE-9B7FE9EF.pf", "MEGASYNC.EXE-A6895B5C.pf", and "VLC.EXE-5F2E6616.pf". The data stored within the Prefetch file "TELEGRAM.EXE-9B7FE9EF.pf" indicates the last eight times the Telegram application was ran by the computer user was between December 30, 2022 and January 3, 2023. Additional, the data stored within the Prefetch file "MEGASYNC.EXE-A6895B5C.pf" indicates the last eight times the Mega Sync application was ran by the computer user was between November 29, 2022 and December 26, 2022.

The 387 Prefetch files are included in **Attachment 10**. **Attachment 11** contains the Prefetch history extracted from the 387 Prefetch files.

7. **Mozilla FireFox**
Mozilla Firefox is a web browser used to access websites and download files on the Internet. Mozilla Firefox stores a record of the users browsing activity in several files, such as "logins.json", "logins-backup.json", and "places.sqlite". These three files were located in the folder "\Users\dbart\AppData\Roaming\Mozilla\Firefox \Profiles\4c57gwra.default-release\". A review of the files "logins.json" and "logins-backup.json" identified the usernames "notfakemail@gmx.com", "I_need_rehab", and "cornercamper" being used to access several websites on the Internet. Some of these websites are "https://accounts.google.com", "https://chaturbate.com", and "https://forums.leakednudes.co".

The files "logins.json", "logins-backup.json", and "places.sqlite" are included in **Attachment 12**. **Attachment 13** contains the extracted browsing and login activity from the files "logins.json", "logins-backup.json", and "places.sqlite".

8. **Password Spreadsheet**
The folder "\Users\dbart\OneDrive\Documents\" contains the Microsoft Excel spreadsheet file "Pass.xlsx". This file has a file creation date of June 4, 2022. A review of the file "Pass.xlsx" identified numerous usernames,

passwords, and the associated website or internet service. Some of these usernames are "dbarte00", "david.m.bartels", and "Notfakemail". Additionally, some of the passwords used to access various websites and internet services appear to be the same across multiple usernames. The file "Pass.xlsx" is included in **Attachment 14**.

ITEM 3: DellLaptop_ToshibaHD1TB (Dell Laptop)

9. **The Onion Router**
The Onion Router, also known as TOR, is a web browser that allow users to access websites on the TOR network. The websites on the TOR network will contain ".onion" at the end of the website address. The TOR browser may store browsing activity in several files, if the user chooses. The folder "\Users\Privacy\Desktop\Tor Browser\Browser\TorBrowser\Data\Browser\profile.default\" and its subfolders contain files related to the TOR browser application. TOR users will typically bookmark TOR website addresses in lieu of storing browsing history. A review of the database file "places.sqlite" identified the following bookmarked TOR websites:
   A. [redacted]guezcinqd.onion/video/1
      a. [Examiner Note: The website title is [redacted]. As of October 24, 2023, this TOR website is still operational and contains CSAM videos for users to view and download. **Attachment 15** contains a screen capture of the TOR website.]
   B. [redacted]7iie7z2wcg.onion/
      a. [Examiner Note: The website title is "[redacted] | The Uncensored Tor Search Engine".]
   C. [redacted]zp4lpc.onion/cat11/
      a. [Examiner Note: The website title is "[redacted]".]

These websites were bookmarked on February 10, 2021. **Attachment 16** contains the TOR database file "places.sqlite". **Attachment 17** includes the extracted bookmarks from the file "places.sqlite".

ITEM 4: EXTRACTION_USERDATA.zip (Samsung Galaxy Z Fold 3)

10. **VLC Player**
The VLC Player stores a record of video and audio files that have been played using the VLC player in the database file "vlc_media.db". This file was located in the folder "/data/data/org.videolan.vlc/app_db/". A review of the database file "vlc_media.db" identified multiple instances in which video files with filenames beginning with the text "Screen_Recording" were viewed by the user. The last play date for these videos range between November 10, 2022 and January 5, 2023. Some of these videos still exist on this Samsung Z Fold in the folder "/data/media/0/DCIM/Screen recordings/". The folder "Screen recordings" contain a total of 254 video files. **Attachment 18** contains the database file "vlc_media.db" and the 254 video files from the folder "Screen recordings". A listing of imported and played video and audio files are included in **Attachment 19**.

11. **Google Play Store**
Google Play is a service created by Google that allow users to browse and download applications from the internet onto their Android devices. The Google Play Store stores a record of applications specific Google user accounts have downloaded in the database file "library.db". The database file "library.db" was located in the folder "/data/data/com.android.vending/databases/". This database also stores the specific "purchase time", indicating the date and time the user downloaded the application.

A review of the database file "library.db" identified 392 Google Play Store installed application entries associated with the Google user account "tacticaldave666@gmail.com", including the applications Telegram, KIK, BIGO, Periscope, Dropbox, Instagram, and TunnelBear VPN.

Attachment 20 contains the database file "library.db". A listing of the Google Play Store installed applications for the Google user account "tacticaldave666@gmail.com" is included in **Attachment 21.**

ITEM 5: WDMyPassport2TB_EXT.E01.E01

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 6: MSILaptop_1TBIntelNVME_1.E01

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 7: MSILaptop_1TBIntelNVME_2.E01

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 8: FujiFilmUSBDrive_16GB.E01

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 9: 61ac799cde43878ac28c419eced7855507196fd0_files_full.zip

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 10: BOBLOV_SanDiskMicroSD256GB.E01

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 11: CleaningUpInLaundromatsCD.iso

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 12: WDEasyStore_5TB.E01

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 13: Kingston128GB_NVME.E01

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 14: SanDiskMicroSD2GB.E01

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 15: MicroSD_15GB.E01

Additional evidence relating to CSAM was not identified on this evidence item.

Subject: Computer Forensic Examination – Investigation of David Bartels	
Examiner: Dero Tucker	**ACTS Number:** 202300569
Case Type: Child Exploitation	**Report Date:** December 4, 2023
Attachments: 21	**Page:** 7 of 7

ITEM 16: SanDiskMicroSD128GB.E01

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 17: SanDiskExtremeProSDCard_32GB.E01

Additional evidence relating to CSAM was not identified on this evidence item.

ITEM 18: WD14TB_WDElementsEXT.E01

Additional evidence relating to CSAM was not identified on this evidence item.

CONCLUSION:

1. The Western Digital 5TB External Hard Drive contains hundreds of images and videos depicting Child Sexual Abuse Material (CSAM) stored in several subfolders of the folder "Deeper". The creation date for these images and videos range between January 11, 2021 and April 18, 2021. The jumplist, Microsoft Internet Explorer, and Microsoft Edge browser activity stored on the MSI Laptop show several of the images and videos were viewed by the user of the MSI Laptop.

2. The "Downloads" folder contains documents pertaining to an individual named "David Bartels". These documents include additional Personal Identifiable Information.

3. The file "Pass.xlsx" located on the MSI Laptop appear to contain usernames and passwords to various websites on the internet. Some of these usernames are "dbarte00", "david.m.bartels", and "notfakemail". Many of the passwords across the usernames are the same or similar.

4. The Onion Router (TOR) browser was installed on the Dell Laptop. The user of the Dell Laptop bookmarked the TOR website "[redacted]gguezcinqd.onion/video/1" on February 10, 2021. This TOR website contains CSAM videos for users to view and download.

DERO TUCKER Digitally signed by DERO TUCKER Date: 2023.12.04 10:12:59 -05'00'

(Signature of examiner) *(Date)*

JAMES FOTTRELL Digitally signed by JAMES FOTTRELL Date: 2023.12.04 10:26:37 -05'00'

(Signature of reviewer) *(Date)*